

CLAIMS

What is claimed is:

1. A web server system for a physical entity, comprising
a web server that generates content regarding the physical entity in response to external requests with the web address of the web server;
a location beacon adjacent to the physical entity to transmit a first beacon signal containing the web address and a token that expires within a predetermined time period;
a location authentication beacon adjacent to the physical entity to transmit a second beacon signal containing the web address and a customized token encrypted using a key;
a location authentication module that retrieves the key from a first request from a client system that has captured the first beacon signal if the first request contains the key and the token that has not expired, and causes the web server to service a second request from the client system if the second request contains the customized token that has not expired.
2. The web server system of claim 1, wherein the location authentication module uses the key to decrypt the customized token in order to authenticate that the second request is indeed from the client system.
3. The web server system of claim 1, wherein the customized token also expires within a predetermined time period, wherein if location authentication module determines that the customized token has expired, then

the location authentication module does not cause the web server to service the second request.

4. The web server system of claim 1, wherein each of the location beacon and the location authentication beacon has a predetermined transmission range.

5. The web server system of claim 1, wherein the key is a random number generated by the client system.

6. The web server system of claim 1, wherein the location authentication beacon further comprises

- a first token generator that generates the un-encrypted customized token using a stored secret key;
- a second token generator that encrypts the customized token using the random number key into the customized token;
- a store that stores the customized token and the web address;
- a communication interface that receives the web address and the customized token from the store and transmits the second beacon signal.

7. A system for authenticating the location of a client system accessing a web server system for a physical entity, comprising

- in the web server system,
 - a location beacon adjacent to the physical entity to transmit a first beacon signal containing a web address of the web server system and a token

that expires within a predetermined time period;

a location authentication beacon adjacent to the physical entity to transmit a second beacon signal containing the web address and a customized token encrypted using a key;

a location authentication module that (1) retrieves the key from a first request from the client system if the first request contains the key and the unexpired token, and (2) causes a web server of the web server system to service a second request from the client system if the second request contains the customized token that has not expired;

in the client system,

a random number generator that generates the key;

a beacon receiver that receives the first and second beacon signals, wherein the beacon receiver generates the first request that includes the key and sends the customized token to a web browser of the client system such that authenticity and location of the client system is verified.

8. The system of claim 7, wherein the location authentication module uses the key to decrypt the customized token in order to authenticate that the second request is indeed from the client system.

9. The system of claim 7, wherein the customized token also expires within a predetermined time period, wherein if location authentication module determines that the customized token has expired, then the location authentication module does not cause the web server to service the second request.

10. The system of claim 7, wherein each of the location beacon and the location authentication beacon has a predetermined transmission range.

11. The system of claim 7, wherein the beacon receiver further comprises

a receiver circuit that receives the beacon signals and parse the tokens from the beacon signals;

a processor coupled to the receiver circuit to control the receiver circuit to either receive the first beacon signal or the second beacon signal;

a request generation module that generates the first request that contains the key.

12. The system of claim 7, wherein the location authentication beacon further comprises

a first token generator that generates a token using a stored secret key;

a second token generator that encrypts the token using the random number key such that the encrypted token becomes the customized token;

a store that stores the customized token and the web address;

a communication interface that receives the web address and the customized token from the store and transmits the second beacon signal.

13. A method of authenticating the location of a client system accessing a web server system associated with a physical entity, comprising transmitting a first beacon signal containing a web address of the web server system and a token that expires within a predetermined time period from

a location beacon adjacent to the physical entity;

generating a random number key in the client system and sending a first request from the client system to the web server system when the client system receives the first beacon signal, wherein the first request contains the web address, the token, and the key;

retrieving the key from the first request in the web server system if the token has not expired and encrypting a customized token using the key;

transmitting a second beacon signal containing the web address and the customized token from a location authentication beacon adjacent to the physical entity;

decrypting the customized token in the client system using the key to determine if the second beacon signal is intended for the client system.

14. The method of claim 13, further comprising
sending a second request to access the web server system if the customized token can be decrypted in the client system using the key, wherein the second request contains the web address of the web server system and the customized token which also expires within a predetermined time period;

causing the web server system to service the second request if the customized token in the second request has not expired;

causing the web server system not to service the second request if the customized token in the second request has expired.

15. The method of claim 14, wherein each of the location beacon and the location authentication beacon has a predetermined transmission range.